3-13-00

PHM 17166

Europäisches Patentamt	European Patent Office	Office européen des brevets

Bescheinigung | Certificate | Attestation

Die angehefteten Unterlagen stimmen mit der ursprünglich eingereichten Fassung der auf dem nächsten Blatt bezeichneten europäischen Patentanmeldung überein.

The attached documents are exact copies of the European patent application described on the following page, as originally filed.

Les documents fixés à cette attestation sont conformes à la version initialement déposée de la demande de brevet européen spécifiée à la page suivante.

Patentanmeldung Nr.	Patent application No.	Demande de brevet n°
	98203638.6	

CERTIFIED COPY OF PRIORITY DOCUMENT

Der Präsident des Europäischen Patentamts:
Im Auftrag

For the President of the European Patent Office

Le Président de l'Office européen des brevets
p.o.

Arlette Fiedler

A. Fiedler

DEN HAAG, DEN
THE HAGUE, 22/03/99
LA HAYE, LE

EPA/EPO/OEB Form 1014 - 02.91

Europäisches Patentamt
European Patent Office
Office européen des brevets

Blatt 2 der Bescheinigung
Sheet 2 of the certificate
Page 2 de l'attestation

Anmeldung Nr.:
Application no.: 98203638.6
Demande n°:

Anmeldetag:
Date of filing: 27/10/98
Date de dépôt:

Anmelder:
Applicant(s):
Demandeur(s):
Koninklijke Philips Electronics N.V.
5621 BA Eindhoven
NETHERLANDS

Bezeichnung der Erfindung:
Title of the invention:
Titre de l'invention:
Proposal for authentication, authorization and accounting based on direct-IP

In Anspruch genommene Priorität(en) / Priority(ies) claimed / Priorité(s) revendiquée(s)

Staat: State: Pays:	Tag: Date: Date:	Aktenzeichen: File no. Numéro de dépôt:

Internationale Patentklassifikation:
International Patent classification:
Classification internationale des brevets:
/

Am Anmeldetag benannte Vertragstaaten:
Contracting states designated at date of filing: AT/BE/CH/CY/DE/DK/ES/FI/FR/GB/GR/IE/IT/LI/LU/MC/NL/PT/SE
Etats contractants désignés lors du depôt:

Bemerkungen:
Remarks:
Remarques:

1. Introduction

Cable Return Channel (CRC) system is a system designed to deliver interactive services to cable *Set Top Boxes* (STB's) and optionally *Cable Modems* (CM's).

Access Service Providers (ASP's) and *Internet Service Providers* (ISP's) strongly require the authentication, authorization and subsequently billing of users entering their networks and using their services respectively.

This document proposes an authentication, authorization and accounting architecture based on the widely used and accepted *Remote Authentication Dial In User Service* (RADIUS) [9], [10] protocol.

The proposal is based on the *Direct-IP* protocol stack which will be mandatory in the next ETS300.800 [1] standard. The current ETS300.802 [2] protocol standard used for DVB compliant interactive services prescribes the use of PPP [4], [6], [7] in the middle layers of the protocol stack between the INA and STB. However, the next version of the ETS300.800 will require a protocol stack for the interaction channel whereby this PPP layer is removed. This protocol stack is called: direct-IP.

1.1 Objectives and Scope

The objective and scope of this document is to propose an authentication, authorization and accounting architecture based on RADIUS for the Cable Return Channel system (CRC system).

The intention of this proposal is to cover the needs of both access service providers and internet service providers.

Intended audience are product managers, architects and, developers that participate in the development of the Interactive Network Adapter (INA) and STB of the interactive cable system.

1.2 References

[1] ETS300800, *Digital Video Broadcasting (DVB); DVB Interaction channel for Cable TV distribution systems (CATV)*, EBU/CENELEC/ETSI-JTC, 12th August 1997

[2] ETS300802, *Digital Video Broadcasting (DVB); Network-independent protocols for DVB interactive services*, EBU/CENELEC/ETSI-JTC, November 1997

[3] Comer, DOUGLAS E., *Internetworking with TCP/IP, Vol 1: Principles, Protocols, and Architecture*, Prentice Hall, Englewood Cliffs, New Jersey

[4] McGregor G., *The PPP Internet Protocol Control Protocol (IPCP)*, RFC 1332, Merit, May 1992

[5] B. Lloyd, L&A, W. Simpson, *PPP Authentication Protocols*, RFC 1334, DayDreamer, October 1992

[6] Simpson, W., *PPP LCP Extensions*, RFC 1570, DayDreamer, January 1994

[7] Simpson, W., *The Point-to-Point Protocol (PPP)*, RFC 1661, DayDreamer, July 1994

[8] Simpson, W., *PPP Challenge Handshake Authentication Protocol (CHAP)*, RFC 1994, DayDreamer, August 1996

[9] C. Rigney Livingston, A. Rubens Merit, W. Simpson Daydreamer, S. Willens Livingston, *Remote Authentication Dial In User Service (RADIUS)*, RFC 2138, April 1997

[10] C. Rigney Livingston, *RADIUS Accounting*, RFC 2139, April 1997

1.3 Acronyms

ASP	Access Service Provider.
BNA	Broadcast Network Adapter.
CM	Cable Modem.
CRC	Cable Return Channel.
DVS	Digital Video Systems.
HFC	Hybrid Fiber Coax.
INA	Interactive Network Adapter.
IP	Internet Protocol [3].
ISP	Internet Service Provider.
MAC	Medium Access Control [1]
RADIUS	Remote Authentication Dial In User Service [9], [10].
RF	Radio Frequency.
STB	Set Top Box.
TCP	Transfer Control Protocol [3].
UDP	User Datagram Protocol [3].

2. Requirements

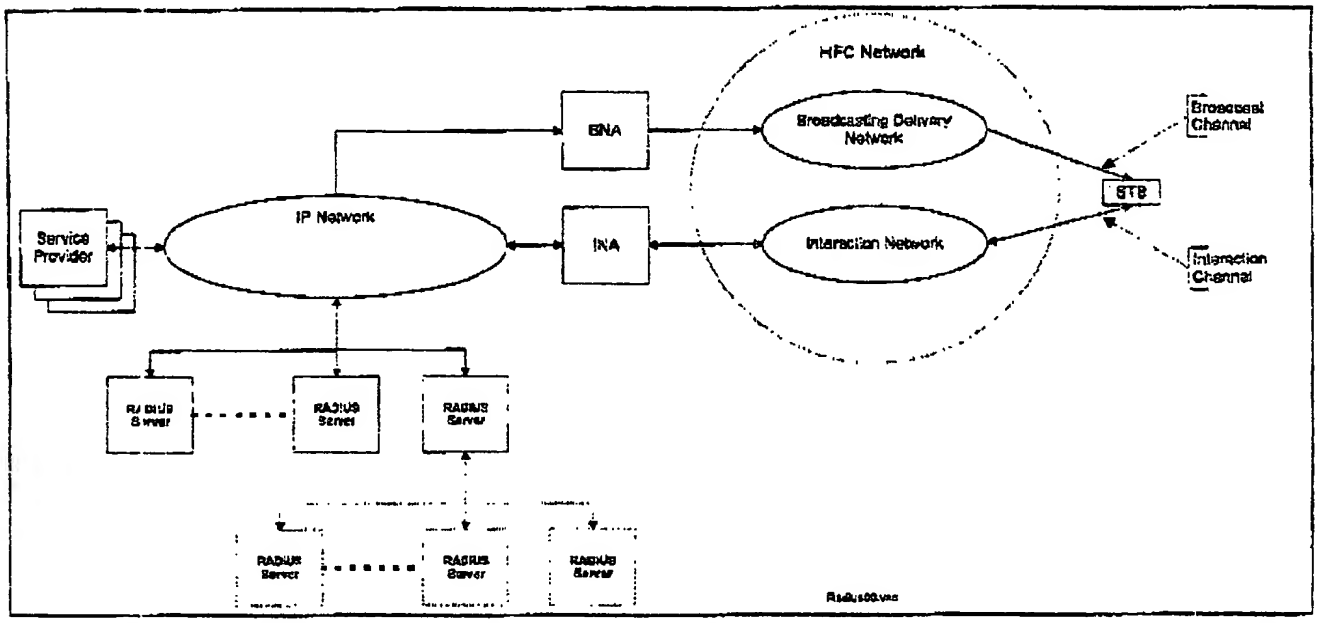
The proposed authentication, authorization and accounting architecture is based on the following requirements:

- The architecture shall be based on the RADIUS [9], [10], as this is the standard for authentication, authorization and accounting within the Internet community.
- The architecture shall offer authentication, authorization and accounting on a per session basis.
- The architecture shall support different applications running in parallel.
- The architecture shall allow the use of different accounting policies e.g. one for *web-browsing* and another for *IP-telephony*.
- The architecture shall allow each ISP or ASP to do its own authentication, authorization and accounting.
- The architecture shall allow STB's which doesn't contain functionality for this architecture to enter the cable network. However, security measures shall be taken that they can not access (accountable) services for which they have to be authenticated and authorized.
- The architecture shall have no impact on the current ETS300.800 [1], ETS300.802 [2] and the next version of the ETS300.800 standards.
- The architecture shall be secure i.e. users can not circumvent authentication, authorization and accounting e.g. by '*hacking*' the STB or CM.
- The architecture shall allow authentication, authorization and accounting for the *interaction network* as well as the *broadcasting* network.

3. System Model

3.1 Reference Architecture

The following diagram presents a block diagram of the reference architecture for authentication, authorization and accounting within the CRC system:



In the reference architecture, two logical channels are established between the STB and service provider: the *broadcast channel* and the *interaction channel*. The unidirectional broadcast channel which is part of the *Broadcasting Delivery Network* includes video, audio and data. The bi-directional interaction channel which is part of the *Interaction Network* is intended for interaction purposes. It is formed by a *return interaction path* and a *forward interaction path*. The forward interaction path maybe embedded into the broadcast channel. It is possible that the forward path of the interaction channel is not required in some simple implementations which make only use of the broadcast channel for carrying data. Physically, the broadcasting delivery network and interaction network are laid over one HFC network i.e. the STB has one RF connection to the HFC network.

The *Interaction Network Adapter* (INA) implements the functionality of a *Network Access Server* (NAS) for allowing STB's and Cable Modems to access the IP network [3] over the HFC network. It embeds the interactive (IP) data in the interaction channel.

The *Broadcast Network Adapter* (BNA) embeds the (IP) data in the broadcast channel.

RADIUS servers are responsible for receiving session requests from the INA, authenticating the STB (i.e. STB session), and subsequently returning all configuration information necessary to deliver the service to the STB in question.

Optionally, a RADIUS server can act as a proxy client to other RADIUS servers or other kinds of authentication servers.

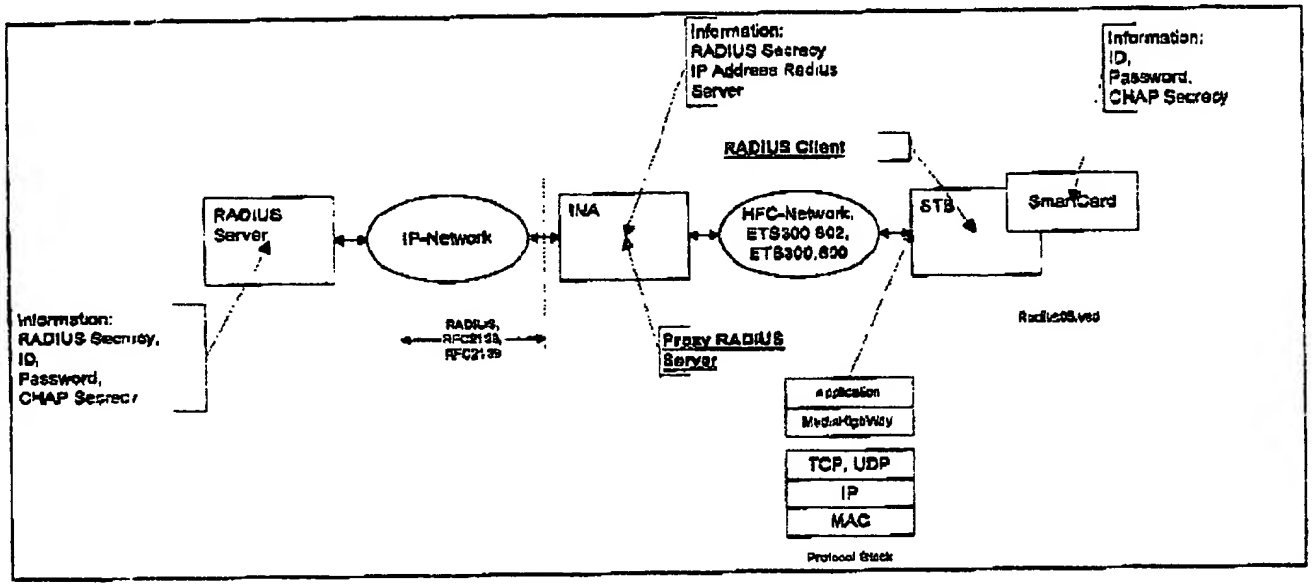
4. Direct-IP based Architecture (Proposal)

The here proposed direct-IP based architecture for authentication, authorization and accounting is a solution for the situation that PPP is removed from the protocol stack. So, PPP can no longer be used for authentication and authorization [5], [8]. This situation will arise with the next version of the ETS300.800 standard wherein, so called: *direct-IP* is mandatory and PPP optional (Subsequently, PPP will be removed from this standard!).

The proposal is to add RADIUS functionality to the Set-Top-Box and Cable Modem i.e. it looks like a *RADIUS client* is built into the STB or CM. This can be done by adding RADIUS functionality to the STB and CM middle ware e.g. *MediaHighWay* layer of Canal+.

4.1 Reference Model

The following diagram presents a reference model for this architecture:



The STB RADIUS client communicates with the RADIUS proxy inside the INA which on its turn communicates with the RADIUS server of the ISP or ASP in question. The INA includes functionality for accounting and an IP filter.

The STB uses a *SmartCard* which contains for each user an ID, password and a CHAP secrecy. At set-up of the connection, this information is used to authenticate and authorize the STB by the RADIUS server.

The INA contains a RADIUS secrecy for securing the connection with the RADIUS server. The RADIUS secrecy is used to add to each RADIUS message a *cryptographic message digest* of the payload of the message, so that the RADIUS server can verify that the message is generated by an authorized INA and not tempered

The data base of the RADIUS server contains for each STB i.e. SmartCard, the ID, password and CHAP secrecy. Furthermore, it contains for each INA the RADIUS secrecy for authenticating the RADIUS messages coming from the INA in question and vice versa.

4.2 STB RADIUS Client

The RADIUS client inside the STB implements all necessary functionality for RADIUS authentication, authorization and accounting. It is capable of generating and handling all RADIUS messages i.e. *Access-Request, Access-Accept, Access-Reject, Access-Challenge* and the accounting messages: *Accounting-Request* and *Accounting-Response* plus the necessary message attributes.

RADIUS messages will only be exchanged on the *Interaction Channel* between the STB and INA.

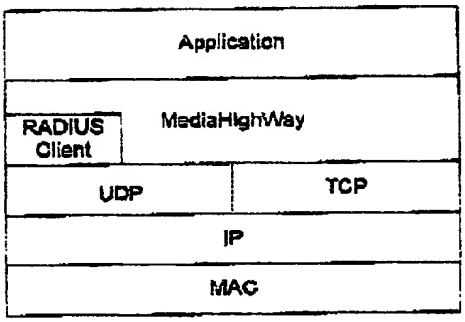
The STB knows the IP address of the RADIUS server, it needs for authorization, authentication and accounting. If this is not the case, the STB uses the IP broadcast address: 255.255.255.255 and the proxy RADIUS of the INA fills in the IP address of the default RADIUS server. (RADIUS uses the well know UDP port number 1812 for RADIUS authentication and authorization and 1813 for RADIUS accounting.)

The RADIUS message attribute: '*NAS-Port*' can be used to address the different STB applications.

The RADIUS message attribute: '*NAS-IP-Address*' is used to inform the designated RADIUS server of the IP address of the RADIUS client i.e. STB.

4.3 STB Protocol Stack

The following protocol stack is used for the direct-IP architecture:



Radius02.vsd

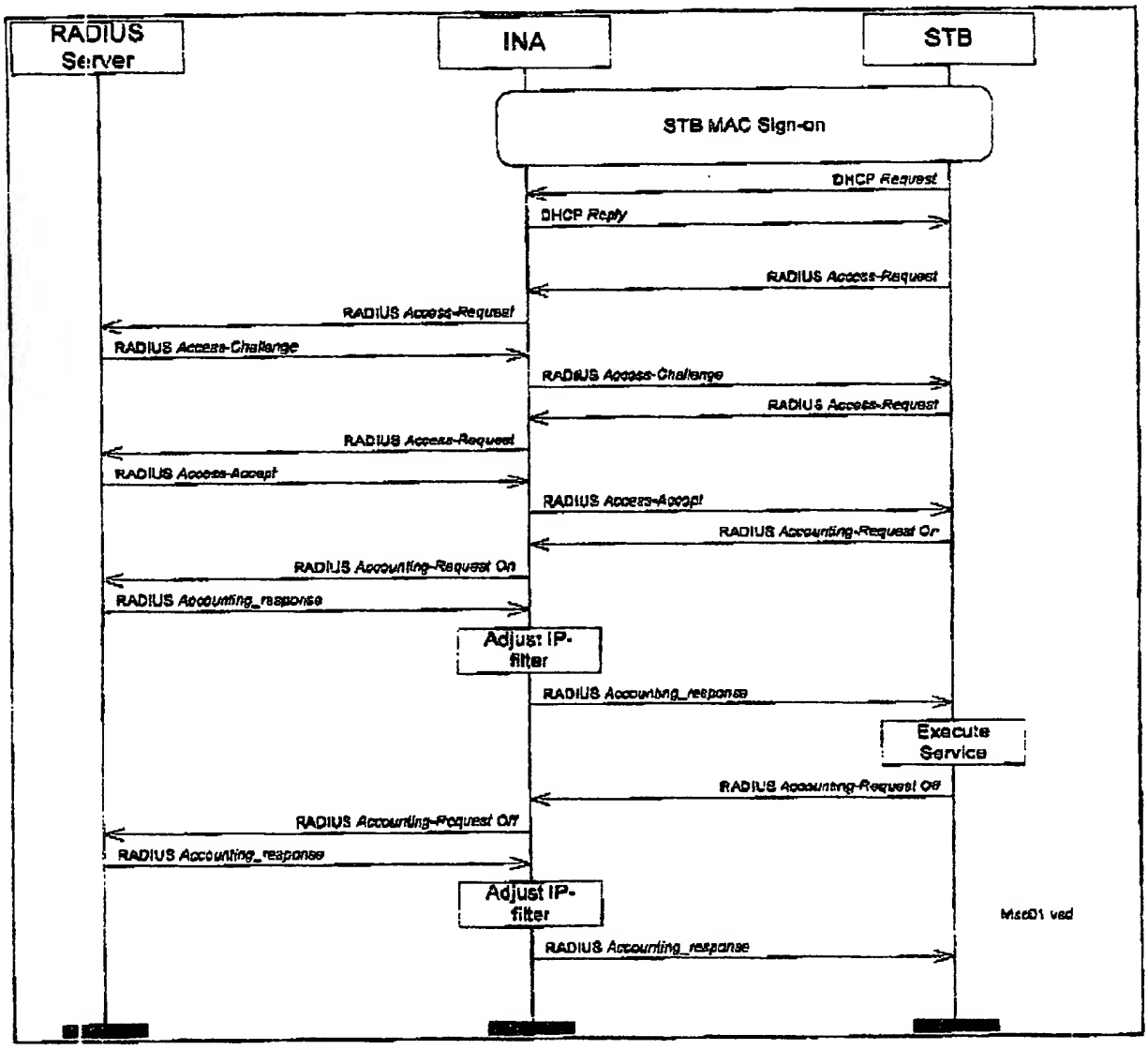
The RADIUS client is on top of UDP/IP [3]. It can be part of e.g. MediaHighWay adaptation layer. More than one STB application can make use of the RADIUS functionality, so that for each application a RADIUS session can be executed i.e. authentication, authorization and accounting can be done.

5. Interactions

The interactions between the RADIUS Server, INA and STB is described with the aid of *Message Sequence Charts* (MSC).

5.1 Normal Authentication, Authorization and Accounting Sequence

The MSC below shows the normal interactions between the STB, INA and RADIUS server for authenticating, authorizing and accounting. This sequence is executed after a STB has successfully signed-on, on MAC layer:



The following steps are executed:

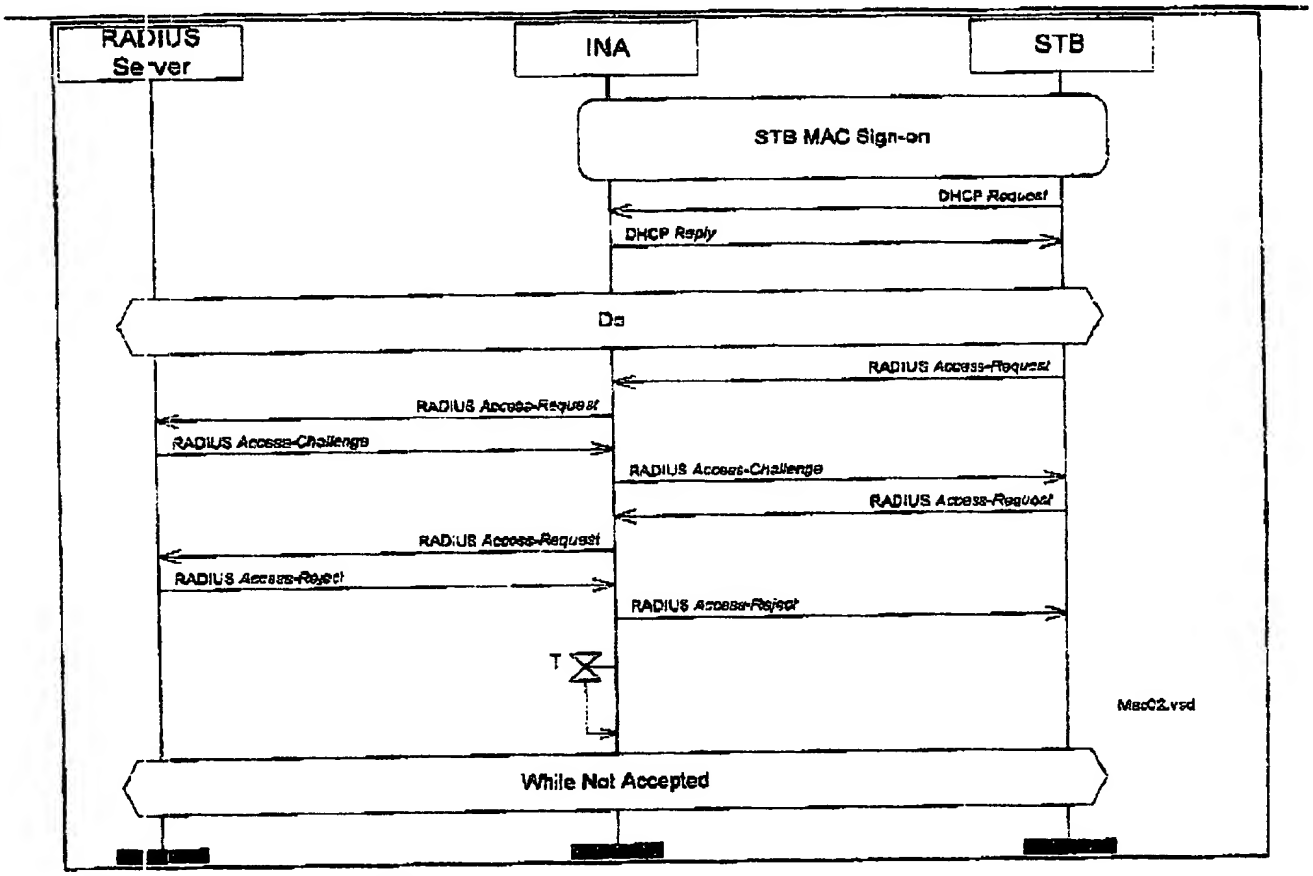
1. The STB sends a DHCP request message to get an IP address.
2. The INA replies with a DHCP reply message containing an IP address to be used by the STB.

3. The STB sends a RADIUS access request message for entering the cable network.
4. The INA forwards this request message to the appropriate RADIUS server.
5. The RADIUS server generates a RADIUS challenge message to authenticate the STB.
6. The STB replies with a RADIUS access request message containing the RADIUS challenge response.
7. If the challenge response is okay, the RADIUS server replies with a RADIUS access accept message. This signals the INA and STB that the STB is allowed to enter the cable network.
8. When the service in question is started, the STB sends a RADIUS accounting request message to turn on the accounting for the service in question.
9. The RADIUS server will respond with a RADIUS accounting response message. This message will adjust the IP-filter of the INA in such way that the IP-datagrams of the service (and STB) in question can be forwarded by the INA.
10. When the service has finished, a RADIUS accounting request message to turn off accounting, is send to the RADIUS server.
11. When the response is received from the RADIUS server, the IP-filter is adjusted in such way that the IP datagrams of the service in question is blocked by the INA.

Note that this is a rough indication of how the interaction between the STB, INA and RADIUS server can be done. Many variations can be introduced on this sequence.

5.2 Rejected STB Sequence

The MSC below shows the interactions between the STB, INA and RADIUS server for the case that the STB is rejected:



The following steps are executed:

1. The STB sends a DHCP request message to get an IP address.
2. The INA replies with a DHCP reply message containing an IP address to be used by the STB.
3. The STB sends a RADIUS access request message for entering the cable network.
4. The INA forwards this request to the appropriate RADIUS server.
5. The RADIUS server generates a RADIUS challenge to authenticate the STB.
6. The STB replies with a RADIUS access request message containing the RADIUS challenge response.
7. When the challenge response is not okay, the RADIUS server replies with a RADIUS access reject message. This signals the INA and STB that the STB is not allowed to enter the cable network.

After some time the STB retries to enter the network again. This can be handy for the case that the access permissions of the STB has changed in the meantime. For example, the user has called the service center of the access service provider to update its permissions.

The IP-filter inside the INA will prevent that unauthorized data enters the cable network.

Note that this is a rough indication of how the interaction between the STB, INA and RADIUS server can be done. Many variations can be introduced on this interaction.

6. Discussion

With PPP, only the PPP '*pipe*' (i.e. connection) is authenticated and authorized. Furthermore, the used accounting is the same for all types of services i.e. it can not support different accounting policies for different services. In the direct-IP architecture, the authentication, authorization and accounting can be done on a per service basis.

By using an IP-filter and by doing accounting outside the STB, the proposed architecture is expected to be secure i.e. users can not circumvent authentication, authorization and accounting by using an '*phony*' STB. The IP-filter will keep out data of unauthorized STB's. The IP-filter will be controlled by the RADIUS messages from the RADIUS server in question.

The proposed architecture can support homogeneous networks with cable modems and STB's from third parties.

(Note that the proposed architecture also works with PPP!)

Claims

1. Communication system comprising a client station being connectable to a server station via a IP based network, characterized in that the communication system comprises authentication means operating at the application layer.

2. Communication system according to claim 1, characterized in that the authentication is based on the RADIUS protocol.

3. Client station for use in a communication system according to claim 1.

4. Server station for use in a communication system according to claim 1.

5. Signal carrying authentication protocol information to be used in the system according to claim 1.